ADMINISTRATIVE DIRECTIVE

SUBJECT **INFORMATION SECURITY POLICY**	NUMBER **1.08-3**	PAGE **1 of 10**
	PAGE ISSUE DATE **July 10, 1996**	

I. PURPOSE

This directive provides policies and procedures for the safeguarding of City electronic information.

II. DEFINITIONS

A. Access - To log into, instruct, communicate with, store in, retrieve from, or otherwise use a computer or City electronic information.

B. Access Key - A configuration of alphanumeric characters used to identify a user.

C. City Manager, Director of Information Technology, and Department Director -- includes those persons and any designee(s) of those persons.

D. City Computer - A computer owned or operated by the City.

E. Computer - Equipment that can perform memory or data processing functions by manipulating electronic, magnetic, optical or other inputs in order to acquire, create, access, modify, store, manipulate, manage, move, control, display, switch, interchange, transmit, process, receive, or produce data or information. The term includes individual computers and any connected system, subsystem, or network of such equipment or devices, including output, processing, storage, memory, software, communications, and other ancillary devices and equipment.

F. City electronic information - Any and all information, data, software, security measures, E-Mail, or other material that is acquired, created, accessed, modified, stored, manipulated, managed, moved, controlled, displayed, switched, interchanged, transmitted, processed, received, or produced electronically.

G. E-Mail - Any system used by the City of Tucson that allows the electronic communication of messages via computer between a sender and one or more recipients, and any message(s) produced through the system. The term "message" includes any attachment(s) to the message. (See also A.D. 1.08-4, "E-Mail.")

H. Firewall - A computing platform or electronic device that serves as a barrier to protect other computing platforms on the network from being directly accessed.

I. Information Security Liaisons - Departmental representatives charged with the responsibility of overseeing the protection of City electronic information.

J. Information Technology Standards Committee - A citywide committee established by the Department of Information Technology to promote consistency in the development and use of the City's computer system.

K. Network - A configuration of computers and software connected for information exchange. Networks may be either LANs (Local Area Networks) that link computers over a short distance, usually less than 10 kilometers, or WANs (Wide Area Networks) that cover larger distances.

L. Password - A string of characters used to gain access to City electronic information.

M. Publicly Accessible Electronic Information - City electronic information that the general public may access on a read only basis.

N. Security measures - Codes, passwords, encryption methodology, hardware, software or other equipment, policies, or procedures that restrict access to a computer or City electronic information, secure the computer or City electronic information from destruction or modification, or otherwise assure the availability, confidentiality, security, and integrity of the computer or City electronic information.

O. Software - includes, but is not limited to, source and object programs, shareware, netware, utilities, diagnostic programs, operating systems, and communication programs.

P. User - Any person or entity who accesses City electronic information.

III. POLICY

As further described in this directive, City electronic information:

- Is the sole property of the City, and users have no personal or property rights in it.
- Shall be protected to ensure the information is available when needed, and is secured from unauthorized access, modification, or release.
- Shall only be released or made accessible to the public by department director approval, in accordance with the Arizona Public Records Act and other applicable laws, and City or department policies.
- Shall, except in the case of publicly accessible electronic information, be accessible to

persons other than City employees only with proper authorization.

IV. GENERAL

A. City Ownership of, and Right of Access to, City Electronic Information

City electronic information is solely the property of the City, regardless of physical location or how maintained; users have no personal property, privacy, or other rights in it.

As owner, the City has at all times the right of access to City electronic information, whether or not it has been made subject to security measures. The City Manager may access City electronic information within any department or office, and department directors may access City electronic information within their respective departments. Where necessary, assistance in obtaining authorized access shall be provided by the Director of Information Technology. Any user shall cooperate in the access of specific City electronic information at any time upon an authorized request.

The accessing of a department's City electronic information shall be coordinated with the department director, unless the City Manager determines that the access should remain confidential.

B. Security of City Electronic Information

All City electronic information, including publicly accessible electronic information as appropriate, shall be secured from unauthorized access, destruction, or modification. All access shall be in compliance with any applicable legal requirements and City and department policies and procedures.

Software and hardware security products selected as standards by the City-wide Information Technology Standards Committee will be used for all computer systems and equipment that contain restricted information. These products will provide for ease of access while still securing the information. Non-standard security products may be authorized by the Department of Information Technology on a case by case basis upon justification by the department requesting the exception.

Criminal justice systems may be subject to special security requirements and standards to ensure confidentiality of information. Access by employees and non-employees to criminal justice information maintained on City computers will be as authorized by the Police Department or City Court, in conformance with legal requirements for release of such information.

C. Release of City Electronic Information to the Public

Release of City electronic information to the public, including both release in response to public records requests and the categorization of City electronic information as publicly accessible electronic information, shall be by department director approval, in accordance with the provisions of the Arizona Public Records Act and City or department policies. Any questions concerning release of City electronic information should be directed to the City Attorney's office. The City will determine the form in which City electronic information is to be released, unless the form is specified by law.

Nothing in this directive shall be construed as a statement or admission by the City that any particular City electronic information is in fact subject to disclosure under the Arizona Public Records Act. Such a determination will be made on a case by case basis.

D. Access by Non-Employees to City Electronic Information

Non-employees may not access City electronic information, beyond that which the City has made publicly accessible, unless authorization is obtained from the City as provided below:

1. A department director may authorize persons who are providing services to the department (e.g., consultants or employees of temporary agencies) to access information from a City computer, if such access is necessary to carry out their work assignments on behalf of the City, and consistent with the City's policies and security requirements.

2. A department director may, on a case by case basis and in consultation with the City Attorney's office and the Department of Information Technology, authorize other users, including contractors and governmental agencies, to access City electronic information from a City or a non-City computer, if such access is necessary to carry out the user's work assignments, deemed beneficial to the City, and consistent with the City's policies and security requirements. The user must demonstrate to the City's satisfaction that the City electronic information will remain confidential, and will be protected by adequate security measures.

E. Distribution of Directive and Compliance with Requirements

Departments shall provide a copy of this directive to all computer users. Users shall comply with the provisions of this directive, and shall be subject to penalties for failure to comply with any requirement.

In addition to civil or criminal remedies or sanctions available to the City under law, penalties for violation of this directive may include:

For City employees, appropriate disciplinary action, up to and including termination.

For non-employees, immediate loss of the privilege to use any City computer and City electronic information, and other sanctions available to the City, such as contract revocation.

V. RESPONSIBILITIES

A. Department of Information Technology Responsibilities

Security issues posed by the implementation of networks are City-wide in scope, since breaches of security on networked devices may present risks to other resources on the network. Inter-network connections to other agencies, the Internet, and dial-up remote access can present serious threats to the security of the entire network. The Department of Information Technology is responsible for maintaining security at the City network level, and shall provide oversight, design, and administration for resources which impact network security.

B. Departmental Responsibilities

Since departments are most familiar with their information processing, they are best qualified to identify their City electronic information and indicate how and to what extent it should be secured, based upon legal considerations or departmental policies, and assistance, upon request, from the Department of Information Technology.

1. Each department shall secure its City electronic information from unauthorized access, destruction, or modification; prevent unauthorized access to its computers; dispose of unnecessary information in accordance with A.D. 1.05-1 ("Records Management Policy")**;** monitor user compliance with security procedures; and restrict access to confidential information (e.g., computerized employee information) to those users whose duties require access.

2. Each department shall develop a plan for securing its City electronic information. The following steps should be used by departments in developing a plan:

- Evaluate all City electronic information as to the importance of its availability, confidentiality, and protection from unauthorized changes.
- Determine the probability that losses will occur.
- Evaluate the economic impact from such losses.
- Recommend the most acceptable method of security commensurate with the amount of risk and the cost of securing the information.

Working together, departments and the Department of Information Technology will review the plan and implement appropriate security measures to accomplish the purposes of this policy.

3. Departments shall monitor implementation of the security procedures, including compliance with file backup procedures.

4. To ensure that the City's computers and electronic information are not subject to modification by former users who should no longer have access:

- The Department of Human Resources shall inform the Department of Information Technology of all employee resignations and terminations.

- Each department shall notify the Department of Information Technology when any contract personnel or consultants, who have been authorized access to computer systems managed by Information Technology, have completed their service to the City.

- Should a department desire to temporarily limit an employee's access (e.g., when the employee is on an extended leave of absence or suspension), the Department of Information Technology shall also be notified.

C. User Responsibilities

1. Users shall assist in maintaining the security of City electronic information, through the steps set forth in this directive.

2. Except where designated as publicly accessible, City electronic information shall be accessed only for official City business and purposes, and for such other activities as may be necessary and desirable to meet City organizational needs and goals. Access for other purposes is prohibited.

3. City employees, and non-employee users authorized to access City electronic information pursuant to Section IV.D, shall not access or attempt to access City electronic information except where necessary to the performance of their work assignments. This section shall not be construed to prohibit the use of training or tutorial software or similar activities that may improve users' ability to carry out their work assignments.

4. Persons using publicly accessible electronic information shall not attempt to circumvent security measures relating to such information, nor take other action that might compromise the availability, security, or integrity of that information.

5. A user's personally owned software or hardware shall not be installed on any city computer except as provided under Section VI.C.

6. Users shall not attempt to obtain information regarding any security measure(s) for computers or City electronic information to which they do not have authorized access.

7. Except as may be necessary to permit access by authorized City personnel, users shall not share information regarding the security measures that protect computers or City electronic information relating to their work assignment without the prior consent of the director of the department providing access to the user.

8. E-Mail is a form of City electronic information that is governed by the provisions of this directive, as applicable, and the policies and procedures in A.D. 1.08-4, "E-Mail". Should there be a conflict between the two directives, the provisions of A.D. 1.08-4 shall take precedence with regard to E-Mail.

D. Information Security Liaison Responsibilities

Security of City electronic information will be overseen by Information Security Liaisons appointed by each department. The Security Liaisons, in sessions facilitated by the Department of Information Technology, will assist in the development, maintenance, and monitoring of security measures within their departments. The Information Security Liaisons are responsible for authorizing access keys, and ensuring that security measures consistent with this directive are used by employees in their department. Should a Security Liaison be transferred or unable to perform the duties of the position, the director will immediately assign a replacement.

Information Security Liaisons, together with appropriate personnel from the Department of Information Technology, will meet together from time to time as the “Information Security Committee.” This committee will review security policies and procedures and make appropriate recommendations.

VI. SECURITY MEASURES

A. Normal security measures for City electronic information include locked desks, filing cabinets, and offices; password access to resources beyond the desktop workstation; file backups; effective scanning for viruses; establishment of standards, rules and procedures for access to systems; and assurance that the appropriate personnel deal with systems.

Further security measures may be necessary as the availability, integrity, or confidentiality of automated system data becomes more important to regular operations. Attachment A shows further security measures that can be taken to provide for stricter control of data.

B. Virus protection shall be utilized on all City computers. When a virus is detected, the department security liaison shall immediately notify the Department of Information Technology Security Liaison, who in turn is responsible for notifying all departments.

Since viruses can easily spread, removal shall be coordinated through the Department of Information Technology in order to guarantee complete removal of the virus from all City computers. The Department of Information Technology has responsibility for the final determination of appropriate virus removal measures.

New virus signature files shall be provided by the Department of Information Technology to the department system administrator who will install the new files and advise the department Security Liaison.

C. To maintain the integrity of City computers and City electronic information, and to protect against introduction of viruses, legally licensed, personal work-related hardware and software can be loaded or installed onto City computers only with written approval from the department director. Upon receipt of the written approval, the Department of Information Technology will load or install the software or hardware.

D. Mission critical files shall be backed up in accordance with established department guidelines, and the backup secured in a location sufficiently separate from the primary storage device to provide for the recovery of lost or damaged files.

E. A backup strategy for non-critical personal PC files on a LAN PC could be multiple backups. For example, users may wish to back up files to the department 'I' drive (on the network server) daily, and to a floppy disk weekly.

F. To the extent possible, publicly accessible electronic information will not be encumbered by onerous access controls. However, firewall systems will be implemented to separate it from other City electronic information requiring a greater level of control.

G. Access to City electronic information by authorized employees or non-employee users shall occur through access keys, passwords, and other suitable security measures. Security measures, including virus protection, will be regularly reviewed, and changed as often as deemed necessary by the department to protect the security of its City electronic information.

H. Dial-in and dial-out access to or from any network-connected device will occur only through a single centrally-administered remote access modem pool. Other modems may be used only with standalone devices. Exceptions will be made only in cases where adequate security controls are in place to prevent access to resources other than those intended. Such exceptions will require the approval of the Director of Information Technology.

I. All connections to non-City networks will be secured by firewalls designed to permit users with specific needs to access only those resources necessary.

Access to the Internet by City employees will be subject to authorization by their department director, based on business need.

VII. APPENDIX

Attachment A: Security Measures

VIII. RESPONSIBILITY FOR REVIEW

The Department of Information Technology and the Information Security Committee shall review this policy in October of each year, or as necessary.

AUTHORIZED:

CITY MANAGER

SECURITY MEASURES

There are many kinds of security measures that can be taken to provide control of electronic information. Some are more restrictive than others, and more than one can be used where applicable. Listed below are commonly used controls to safeguard electronic information so that it is available when needed (availability), allows only authorized changes to be processed (integrity), and it is accessed only by those with authorization (confidentiality).

Any or all of these measures may be appropriate under given circumstances. Within each category below, the controls are generally ordered from less secure, less costly controls to more secure, more costly controls.

Security Measures to Protect Availability of Electronic Information

- Compliance with retention schedule time frames
- Multiple backups of files
- Off-site storage of backup files
- Cross training of personnel
- Contingency plan for system failure
- Alternative processing sites
- Active hot site

Security Measures to Protect Integrity of Electronic Information

- Control access to server files
- Verify and monitor system usage
- Audit accuracy of electronic information
- Password encryption
- Use of a firewall
- Isolation of computer systems and networks

Security Measures to Protect Confidentiality of Electronic Information

- File access log
- Read access authorization
- Use of a firewall
- Isolation of computer systems and network
- Encryption of electronic information